Information Security in an Academic Environment

Troy Palmer, Lead InfoSec Engineer, CUNY

And

Michael D’Amico, Senior Auditor, CUNY

Who We are

- Troy Palmer, CISSP, Lead Information Security Engineer with CUNY for the past 6 years, 18 Years in Information Security Field, worked in various Governmental Organizations, and Corporate world.

- Michael D'Amico, CISSP, CISA, Senior Auditor with CUNY for the past 7 years, 13 years in information Technology Auditing, worked for Office of the State Comptroller for the State of NY.

What is Academic Freedom?

Academic Freedom Definition

- The Declaration considers the functions of an academic institution, which are (a) to promote inquiry and advance the sum of knowledge; (b) to provide instruction to students; and (c) to develop experts for public service. It argues that performance of each of those functions requires faculty to have complete freedom to pursue their investigations and discuss and publish their results and to express themselves fully and frankly both to their students and to the public.

Source: http://www1.cuny.edu/mu/vc_la/2012/01/02/a-guide-to-academic-freedom/

So how do we work within the confines of Academic Freedom??

Academics vs Administration

- Academics
  - Pursue research unfettered
  - Ease of access to IT resources
  - Security is a burden
  - Unfettered access to student records
  - Mobile access to information from any location (unlimited devices)

- Administration
  - Information technology with ease of use
  - Wants security when convenient
  - Unfettered access to all information
    - No separation or segregation of information (PII/NPUI)
  - Mobile access to information from any location

Academic Controls

- CUNY policy states that CUNY will monitor the network for malicious activity, network intrusions, malware propagation and various other violations of the Acceptable Use Policy
- Monitoring of access/granting of access to various departmental information and resources
- Constant Security Awareness on how to safely use the internet and CUNY resources

Mitigation Controls

- Constant firewall, IPS/IDS, and Malware monitoring
- Network level profiling of systems/hosts to ensure appropriate use of resources
- Host based security tools to help in identification and remediation of host based malware/Internet violations

Administrative Controls

- Risks
  - Non-segregation of duties
  - Loosely controlled system access
  - Improper storage or transmission of sensitive information
    - PII/NPUI
  - Improper use of resources
  - In-ability to use web-filtering tools

- Mitigation
  - Network profile monitoring
  - VPN for offsite or mobile connections
  - Secure transfer protocols for sending of sensitive information
  - Vulnerability assessments
  - Constant firewall, IPS/IDS, and Malware monitoring

Segregation of Duties

- Education of internal controls
- Bi-annual access audits
- Select targeted access audits of high risk roles
- Various spot-checks to help identify issues and non-compliance
- Partnership with Information Security Managers and Business Process Owners to ensure compliance

Internet controls

- Internet of Things (IOT's)
  - A growing base of devices that are placed on the Internet to communicate with other Internet attached devices
- Shodan.io
  - A website that is the "First search engine for Internet connected devices"
  - It further identifies any internet facing devices and the type of protocols used on those said devices
    - Identifies hosts, ports defined to specific applications and versions of software used
    - Available to anyone who uses Shodan and does a search
    - Based on IP range, protocol, or application in use

Source: https://www.shodan.io/

Network Controls

- Firewalls
  - Used to separate and segment portions of the network, create a barrier between CUNY and Internet
- IPS
  - Intrusion Prevention System/Intrusion Detection System
    - Placed in between the Firewall and the inside of an organization
    - Used to detect and prevent malicious activities from the Internet into CUNY as well as from Inside to Campuses
- Profiling
  - Used to detect abnormalities on the network to include servers, workstations and student systems
- Vulnerability Assessments
  - Used to identify and track highly vulnerable systems that require human intervention to reduce their vulnerability footprint
    - Can require the assistance of IT Audit to ensure Campus compliance

Summary

- There’s a lot of work to be done
- Academic Freedom sometimes hinders Information Security/IT Audit from doing its job
- Staffing is sometimes challenging
- Partnership between Information Security and IT Audit to successfully mitigate issues and ensure that the various campuses are compliant
- Some newer technologies can impede controls being used

Questions???